UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/813,533	03/19/2001	Seiichiro Tamai	NAK1-BO25	3576

21611 7590 03/23/2004

SNELL & WILMER LLP
1920 MAIN STREET
SUITE 1200
IRVINE, CA 92614-7230

EXAMINER	
SIANGCHIN, KEVIN	

ART UNIT	PAPER NUMBER
2623	4

DATE MAILED: 03/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/813,533	Applicant(s) TAMAI, SEIICHIRO	
	Examiner Kevin Siangchin	Art Unit 2623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 March 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

Drawings

Objections

1. Figures 1A-1B should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claims

Objections

2. Claim 5 is objected to because of the following informalities. Claim 5 recites, "The identity verification apparatus in Claim 4, wherein the body part is an iris, ... and the motion detection means ... detects movement of the *body* ...", where the applicant intended to recite, "The identity verification apparatus in Claim 4, wherein the body part is an iris and the motion detection means ... detects movement of the *body part* ...". Appropriate correction is required.

Rejections Under U.S.C. § 102(b)

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-2, 6, and 27-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Flom et al. (U.S. Patent 4,641,349).

5. *The following is in regard to Claim 1.* Flom et al. disclose an iris recognition (based on the biometrics of the human iris) comprising the following:

a. A scanning means (i.e. the scanning camera 180 depicted in Flom et al. Fig. 10) for obtaining an image of the iris (note that, henceforth in this document, the iris image will be referred to interchangeably as the object image when the distinction as such is unimportant) by scanning an eye (note that, henceforth in this document, the eye will be referred to interchangeably as the body part when the distinction as such is unimportant) of a person without physical contact. Notice, from Flom et al. Fig. 8, for example, that the scanning of the iris occurs without physically contacting the eye.

b. An image display means (i.e. display screen 86 shown in Fig. 9 of Flom et al.) for displaying the object image to the person. See Fig. 9 of Flom et al. and column 9, lines 27-65.

c. A verification start command receiving means for receiving a verification start command from the person. The process of verification in Flom et al.'s recognition system commences, automatically (e.g. as shown in steps 44-52 in Flom et al. Fig. 4 or steps 352-354 in Fig. 12) or manually (e.g. Flom et al. column 9, lines 61-65), when the size of the iris dilates or contracts to a predetermined size. In this manner, a verification start command is issued, indirectly, when the iris of the subject is of the predetermined size or, directly, when the operator manually commences the verification process. In either case, in order to accommodate such actions, the verification system of Flom et al. must inherently include a verification start command receiving means for receiving a verification start command from the person.

d. A verification means for, when the verification start command is received, extracting biometric information describing a form characteristic of the body part from the object image (e.g. Flom et al. Fig. 7 step 64), and verifying identity by comparison with stored reference biometric information (e.g. Flom et al. Fig. 4 step 66). Refer also to Flom et al. Fig. 12.

It has thus been shown that the iris verification system of Flom et al. is indeed an identity verification apparatus based on biometrics that conforms to claim 1. In this way, the teachings of Flom et al., regarding their iris verification system, anticipates the identity verification system put forth in applicant's claim 1.

6. *The following is in regard to Claim 2.* . Flom et al. disclose an iris recognition (based on the biometrics of the human iris) comprising the following:

a. A scanning means (i.e. the scanning camera 180 depicted in Flom et al. Fig. 10) for obtaining an image of the iris (note that, henceforth in this document, the iris image will be referred to interchangeably as the object image when the distinction as such is unimportant) by scanning an eye (note that, henceforth in this document, the eye will be referred to interchangeably as the body part when the distinction as such is unimportant) of a person without physical contact. Notice, from Flom et al. Fig. 8, for example, that the scanning of the iris occurs without physically contacting the eye.

b. An image display means (i.e. display screen 86 shown in Fig. 9 of Flom et al.) for displaying the object image to the person. See Fig. 9 of Flom et al. and column 9, lines 27-65.

c. A guide display means (i.e. display screen 86 shown in Fig. 9 of Flom et al.) for displaying a guide layered over the object image (i.e. reference number 30 in Flom et al. Fig. 9), the guide showing an outline of the body part in proper position. Reference number 30 is an outline of the pupil of the subject's eye. The peripheral points 88a and the center point 88b are used to align the subject's eye in a standardized position. This is discussed in Flom et al. column 9, lines 23-41.

d. A judgment means for judging whether the object image was scanned in the proper position. In the iris recognition system of Flom et al., the pupil outline 30 superimposed upon the image display screen 86, as illustrated in Flom et al. Fig. 9, allows the operator to judge whether the subject's eye, and hence the subject's iris, is in the proper, standardized position. In this way, these items (i.e. pupil outline 30 and display screen 86) taken together represent a judgment means for judging whether the iris was scanned in the proper position.

e. A verification means for extracting biometric information describing a form characteristic of the body part from the object image, if in the proper position, (e.g. Flom et al. Fig. 7 step 64), and

verifying identity by comparison with stored reference biometric information (e.g. Flom et al. Fig. 4 step 66). Refer also to Flom et al. Fig. 12.

It has thus been shown that the iris verification system of Flom et al. is indeed an identity verification apparatus based on biometrics that conforms to claim 2. In this way, the teachings of Flom et al., regarding their iris verification system, anticipate the identity verification apparatus put forth in applicant's claim 2.

7. *The following is in regard to Claim 6.* As just shown, Flom et al. disclose an identity verification apparatus that conforms to claim 2. The identity verification apparatus of Flom et al. further includes a repetition control means for controlling the scanning means in order to repeatedly scan the iris. This is evident from Flom et al. Figs. 4 and 12. Note in these figures the loop having the loop index n (e.g. the loop formed between steps 42 and 54 in Flom et al. Fig. 4). Further observe that contained in these loops is the step of obtaining an image of the iris. Thus, the iris verification system of Flom et al. includes a repetition control means for controlling the scanning means in order to repeatedly scan the iris. Repetition control is provided by incrementing n and comparing it against a predetermined number N.

8. The verification means of Flom et al.'s identity verification apparatus also operates by extracting biometric information from a plurality of object images obtained by repeated scanning and verifying identity. This is explained in Flom et al. column 11, lines 56-67 to column 12, lines 1-10. It has thus been shown that the iris verification system of Flom et al. is indeed an identity verification apparatus based on biometrics that conforms to claim 6. In this way, the teachings of Flom et al., regarding their iris verification system, anticipate the identity verification apparatus put forth in applicant's claim 6.

9. *The following is in regard to Claims 27-28.* These claims recite substantially the same limitations as claim 2. Therefore, with regard to claims 27-28, remarks analogous to those presented above with regard to claim 2 and are applicable.

10. Claims 18 is rejected under 35 U.S.C. 102(b) as being anticipated by Itsumi et al. (U.S. Patent 5,559,504).

11. *The following is in regard to Claim 18.* Reference is made to Fig 26 of Itsumi et al. depicting the internal circuitry of the IC card with fingerprint identification depicted in Itsumi et al. Figs. 24-25. A detailed description can

be found in Itsumi et al. column 14, line 60 to column 15, line 48. This card (clearly portable) is used for identity verification based on the biometrics of a fingerprint. It comprises a biometric information storage means (i.e. FINGERPRINT DATA REGISTRATION MEMORY 74) for storing reference biometric information describing a form characteristic of a body part, an image data obtaining means (i.e. FINGERPRING INPUT UNIT) for obtaining image data from outside describing a fingerprint, and a verification means (i.e. circuit elements 71, 72, and 77) for extracting biometric information describing a form characteristic of the body part from the object image (see Itsumi et al. column 15, lines 15-27) and verifying identity by comparison with stored reference biometric information (see Itsumi et al. column 15, lines 28-32). It has thus been shown that the iris verification system of Flom et al. is indeed a portable card for identity verification based on biometrics that conforms to claim 18. In this way, the teachings of Itsumi et al., their IC card, anticipate the portable card for identity verification based on biometrics put forth in applicant's claim 18.

Rejections Under U.S.C. § 103(a)

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Ito (U.S. Patent 6,526,160).

14. *The following is in regard to Claim 3.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. In addition, Flom et al. suggest that, in order to automatically align the image of the iris, an automatic alignment system be used to adjust the position of the scanning camera. See Flom et al. column 10, lines 56-65. While such a system clearly represents a scanning control means for controlling the scanning direction, Flom et al. do not suggest the magnification of the scanning camera be adjusted.

15. Cameras that have automatic magnification adjustment are well known. For example, Ito discloses an iris recognition system utilizing a zoom-camera capable of self-adjusting its magnification (zoom), focus and scanning direction based on the position and alignment of the subject's iris. See Ito Fig. 1 and 13, column 9 lines 1-30, and column 9, lines 63-67 to column 10, lines 1-11. Note that the position of the mirror 8c in Ito Fig. 1 dictates the scanning direction of the zoom-camera.

16. It should be clear that the systems depicted in Fig. 1 of Ito and Fig. 8 of Flom et al. are structurally and functionally similar. This implies that a zooming camera and its associated controlling mechanism, such as those taught by Ito, would likely be compatible with the iris detection system of Flom et al. Therefore, it would be straightforward for one of ordinary skill in the art to incorporate a zoom-camera and the mechanism controlling it into an iris recognition system, such as that of Flom et al. This can be easily accomplished, in the recognition system of Flom et al., by either extending the operation of the aforementioned scanning control means and scanning camera to include a zooming feature sensitive to the position of the subject's eye or to replace the Flom et al.'s scanning camera and associated control means entirely with those of Ito. Clearly, having a zooming capability in an iris recognition apparatus, such as that of Flom et al., provides better isolation of the subject's iris and, moreover, a more detailed and accurate image of the subject's iris. Given the advantages of incorporating a zooming (magnification) facility in an iris recognition apparatus and the relative simplicity with which such an incorporation can be made, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to incorporate a zooming feature into the scanning control means of Flom et al. either by extending the operation of the aforementioned scanning control means and scanning camera to include a zooming feature sensitive to the position of the subject's eye, as suggested by Ito, or to replace Flom et al.'s scanning camera and associated control means entirely with those of Ito. By modifying the iris recognition system of Flom et al., in this manner, one obtains an identity verification apparatus that satisfies all limitations of claim 3.

17. Claims 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Steinberg et al. (U.S. Patent 6,433,818).

18. *The following is in regard to Claim 4.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. However, Flom et al. do not a motion detection means for controlling the scanning means, in order to repeatedly scan the body part, and detecting movement of the body from a plurality of object images obtained by repeated scanning. While it was show above, with respect to claim 2, that the iris detection system of Flom et al. includes a judgment means judging that the body part is scanned in the proper position and the verification means verifying identity when the motion detection means detects movement of the body, Flom et al. do not show that this judging and verification should occur after the motion detection means detects movement based on a plurality of images.

19. Steinberg et al. disclose a digital camera with a built-in apparatus for acquiring and verifying biometric data of a potential user. One such apparatus, illustrated in Steinberg et al. Fig. 11, involves the acquisition of a user's iris. It should be clear from Steinberg et al. Fig. 11 that this embodiment of Steinberg et al.'s apparatus for acquiring and verifying biometric data of a potential user is similar, in form and function, to the iris verification system of Flom et al. As shown in Steinberg et al. Fig. 7 and detailed in column 8, lines 44-60, the iris acquisition and verification apparatus of Steinberg et al. includes a motion detection means (apparent from Steinberg et al. Fig. 7, step 198) for detecting movement of the eye – specifically, the dilation and/or constriction of the subject's pupil. The motion detection is predicated on a plurality of images acquired at regular time intervals. Furthermore, the verification proceeds (Steinberg et al. Fig. 7, step 112) only when the motion detection means has detected movement (Steinberg et al. Fig. 7, step 202). As shown in Steinberg et al. Fig. 7, motion detection follows the acquisition of the iris image, which, as indicated Steinberg et al. column 6 lines 17-35 and column 7 lines 5-27, is preceded by some alignment of the eye with respect to the image capturing mechanism. Note that, since the motion detection requires scanning the eye, which further requires the illumination of the eye, the motion detection means of Steinberg et al. will, for the purposes of this document, be taken to be the entirety of Steinberg et al. Fig. 11 (not including the eye, of course) and, correspondingly, steps 106-202 of Steinberg et al. Fig. 7.

20. It should be clear from Steinberg et al. Fig. 11 that this embodiment of Steinberg et al.'s apparatus for acquiring and verifying biometric data of a potential user is similar, in form and function, to the iris verification system of Flom et al. Given these similarities and that Steinberg et al. have successfully incorporated, into an iris recognition apparatus, a motion detection means for detecting the variation in the size of a subject's iris, it would be

a simple undertaking for one of ordinary skill in the art to incorporate a motion detection means, as taught by Steinberg et al., into the iris recognition system of Flom et al. Similarly, it would be straightforward for one of ordinary skill, provided the teachings of Steinberg et al., to incorporate the motion detection means into the iris recognition system of Flom et al. in such a way that the verification occurs after motion has been detected and the motion detection occurs after the image has been aligned (deemed to be in the proper position) with respect to the image capture mechanism (i.e. the scanning camera 180 depicted in Flom et al. Fig. 10). As indicated by Steinberg et al. (Steinberg et al. column 8, lines 44-49), this advantageously allows the recognition system or apparatus to distinguish between non-living, "imposter" subjects and living subjects. This, in turn, provides an additional layer of security. Given the advantage of using such a motion detection scheme in an iris detection apparatus and the ease with which it can be incorporated in to such an apparatus, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to incorporate a motion detection means, as taught by Steinberg et al., into the iris recognition system of Flom et al in such a way that the verification occurs after motion has been detected and the motion detection occurs after the image has been aligned (deemed to be in the proper position) with respect to the image capture mechanism (i.e. the scanning camera 180 depicted in Flom et al. Fig. 10). In doing so, one obtains an identity verification apparatus that satisfies all limitations of claim 4. Note that, here, the notion of what constitutes the motion detection means thus obtained is analogous to the way in which the motion detection means was delineated above, with regard to the iris verification apparatus of Steinberg et al. That is, the motion detection means of the identity verification apparatus, obtained by combining the teachings of Flom et al. and Steinberg et al. in the manner just described, will be taken to include all elements of the identity verification apparatus not involving verification of the iris[1].

21. *The following is in regard to Claim 5.* As just shown, the teachings of Flom et al. and Steinberg et al., when combined in the manner discussed above, address all limitations of claim 4. Notice that both Flom et al. and Steinberg et al. disclose *iris* recognition apparatuses. Furthermore, notice that the light sources 78a and 78b of Flom

1 Therefore, with regard to the teachings of Flom et al., such a motion detection means would include the entirety of Flom et al. Fig. 8 (not including the eye, of course) and, correspondingly, reference numbers 70-80 in Flom et al. Fig. 3, and steps 344-366 in Flom et al. Fig. 12.

et al. Fig. 8 and light sources 174, 176, and 178 in Fig. 11 illuminate the eye throughout the scanning process. See step 354 of Fig. 12 of Flom et al., column 8, lines 55-56 and column 11, lines 34-37. Since the iris is illuminated throughout the scanning process, the scanning means (i.e. the scanning camera 180 depicted in Flom et al. Fig. 10) scans the iris in phase with the illumination. In this way, the teachings of Flom et al. and Steinberg et al., when combined in the manner discussed above, produce an identity verification apparatus in accordance with claim 8.

22. Claims 7-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Fleming (G.B. Patent Application Publication 2,229,305).

23. *The following is in regard to Claim 7.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. As a result, Flom et al. show essentially an identity verification apparatus comprising a *single* body part control means for controlling the scanning means to obtain an object image of each of a *single* body part, causing the image display means to display the object image, causing the guide display means to display the guide image, and causing the judgment means to judge whether the body part is scanned in the proper position, wherein the verification means extracts object biometric information pertaining to the body part from a plurality of object images (see the discussion above with respect to claim 6), and verifies identity by comparing the object biometric information with corresponding reference biometric information. However, Flom et al. do not teach such an identity verification apparatus further comprising a *multiple* body part control means for controlling the scanning means to obtain an object image of each of *a plurality of* body parts, causing the image display means to display the object images, causing the guide display means to display the guide images, and causing the judgment means to judge whether the body parts are scanned in the proper position, wherein the verification means extracts object biometric information pertaining to each body part from a plurality of object images, and verifies identity by comparing the object biometric information with corresponding reference biometric information.

24. Fleming discloses an identity verification apparatus that involves the acquisition and verification of a plurality of physical human attributes, including body parts such as the fingerprint and face. See Fleming Fig. 1.

25. Observe that identity verification apparatus of Fleming shares several of the essential components of Flom et al. including scanning means (e.g. scanners 3 and 4 in Fleming Fig. 1) and a verification means that compares extracted biometric information with stored reference information (e.g. templates 1 in Fleming Fig. 1). Given the fundamental similarities of the two identity verification apparatuses and given the fact that Fleming has shown a way in which to incorporate a plurality of biometric sources into an identity verification system, it would have been straightforward for one of ordinary skill in the art to extend the operation of Flom et al.'s iris verification system to accept and verify biometric information from a plurality of human body parts (e.g. face, iris, and/or fingerprint). It would be clear to one of ordinary skill in the art that, in order to attain the greatest utility from the identity verification apparatus thus obtained, all components of Flom et al.'s iris verification system should be extended (or replicated) to accommodate multiple body parts. In addition to the verification means and scanning means, these components would include the aforementioned image display means, the guide display means, and the judgment means. Clearly, extending the iris detection system of Flom et al., in this manner, to accommodate a multitude of biometric sources, advantageously results in a much more thorough identification of the subject. Given this advantage and Fleming's demonstrated usage of multiple biometric sources in an identity verification system, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to extend the operation of Flom et al.'s iris verification system to accept and verify biometric information from a plurality of human body parts (e.g. face, iris, and/or fingerprint). In doing so, one would obtain an identity verification apparatus, in accordance with claim 2, that accommodate a multitude of biometric sources and further comprises a *multiple* body part control means for controlling the scanning means to obtain an object image of each of *a plurality of* body parts, causing the image display means to display the object images, causing the guide display means to display the guide images, and causing the judgment means to judge whether the body parts are scanned in the proper position, wherein the verification means extracts object biometric information pertaining to each body part from a plurality of object images, and verifies identity by comparing the object biometric information with corresponding reference biometric information. Such an identity verification apparatus is in accordance with all aspects of claim 7.

26. *The following is in regard to Claim 8.* As just shown, the teachings of Flom et al. and Fleming can be combined in such a way as to satisfy all limitations of claim 7. Flom et al. suggest several techniques for

determining the similarity of the captured images of the subject's body part to the stored reference images. One suggested method is the well-known correlation algorithm. See Flom et al. column 7, lines 30-36. It is known that image correlation algorithms yield a measure of the correlation of two images. (Fleming refers to this value as the "score" of the comparison. See Fleming, page 1, lines 11-18.) Flom et al., however, do not calculate a total from a plurality of the correlation values, and verifies identity based on whether the total is greater than a given threshold value.

27. Fleming's verification is predicated on a weighted sum S of the scores S_i obtained by comparing each of the object images, corresponding to each of the subject's body parts, to the stored reference images (templates). See Fleming page 3, lines 13-34 to page 4, lines 1-34. This sum is compared to a threshold to obtain a "pass/fail output". See Fleming, page 3, line 33-34. Note that the scores are the square of the Euclidean distance in pattern space between the unknown pattern and the template. See Fleming, page 3, lines 27-30. Thus, a higher score implies less correlation between the two images. This further implies that a higher S indicates that the subject is more likely to be an imposter. Therefore, while the nature of the comparison between S and the said threshold is not explicitly discussed in Fleming, one can infer that the comparison, and hence the verification, is based on whether the sum S is greater than the given threshold. That is, if S is greater than the subject can be considered an imposter, and if below, the subject is properly identified.

28. The teachings of Flom et al. and Fleming can be combined as shown above. Further incorporating a weighted sum of the correlation values, such as Fleming's S, would be straightforward for one of ordinary skill in the art, particularly since the correlation algorithm suggested by Flom et al. provides a correlative "score". Again, extending the iris detection system of Flom et al., in this manner, to accommodate a multitude of biometric sources, advantageously results in a much more thorough identification of the subject. Given this and the straightforwardness of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to further incorporating a weighted sum of the correlation values, such as Fleming's S, into the identity verification apparatus, obtained by combining the teachings of Flom et al. and Fleming, in the manner described above, with regard to claim 7. In doing so, one would obtain an identity verification apparatus that is in accordance with all limitations of claim 8.

29. *The following is in regard to Claim 9.* As shown above, the teachings of Flom et al. and Fleming can be combined in such a way as to satisfy all limitations of claim 7. Flom et al. disclose an *iris* detection system and Fleming discloses an identity verification apparatus that verifies the identity of an individual based on a multitude of physical human attributes, including a fingerprint. Since the iris and fingerprint are unique to individuals, they are an effective means for identifying an individual. Given this, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to combine the teachings of Flom et al. and Fleming, in the manner described above with regard to claim 7, and to use an iris and a fingerprint as two of the plurality of body parts accepted and verified by the obtained identity verification apparatus. Such an identity verification apparatus would be in accordance with all limitations of claim 9.

30. *The following is in regard to Claim 10.* As shown above, the teachings of Flom et al. and Fleming can be combined in such a way as to satisfy all limitations of claim 7. While neither Flom et al. nor Fleming suggest including a fingerprint from each of a plurality of fingers in the plurality of body parts to be scanned and verified, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to accommodate such an input, particularly given that Fleming's teachings show the use of fingerprint verification and are not constrained to the set of biometric sources depicted in Fleming Fig. 1 and discussed in Fleming's disclosure (see paragraph 1 on page 1 of Fleming). Allowing the identity verification apparatus, obtained by combining Flom et al. and Fleming's teachings in the manner described above, to accept a fingerprint from each of a plurality of fingers simply makes the identity verification more thorough and also introduces an advantageous level of redundancy to account for the possibility of faulty fingerprint verification.

31. *The following is in regard to Claim 11.* As shown above, the teachings of Flom et al. and Fleming can be combined in such a way as to satisfy all limitations of claim 7. While neither Flom et al. nor Fleming suggest including two irises in the plurality of body parts to be scanned and verified, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to accommodate such an input, particularly given that Flom et al.'s teachings are directed to iris verification and the fact that Fleming's teachings are not constrained to the set of biometric sources depicted in Fleming Fig. 1 and discussed in Fleming's disclosure (see paragraph 1 on page 1 of Fleming). Allowing the identity verification apparatus, obtained by combining Flom et al. and Fleming's teachings in the manner described above, to accept two irises simply makes the identity verification

more thorough and also introduces an advantageous level of redundancy to account for the possibility of a single faulty iris verification.

32. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Brown et al. (U.S. Patent 6,618,806).

33. *The following is in regard to Claim 12.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al., however, do not show or suggest that the identity verification apparatus should further comprise an ID data obtaining means for obtaining object ID data to verify a person's identity incident to scanning, wherein the verification means verifies identity by comparing a combination of the extracted biometric information and the object ID data with a combination of the corresponding reference biometric information and reference ID data.

34. Brown et al. disclose a biometric authentication system that includes obtaining ID data (i.e. user ID and password) to initially verify a user's identity prior to and concomitantly with the acquisition of the user's biometric information (Biometric Identifier Record – BIR). See Brown et al. Fig. 3 and column 4, lines 60-67 to column 5, lines 1-25. A reference BIR is retrieved from a database, consisting of a plurality of reference BIRs (Brown et al. column 4, lines 1-3) according to the supplied ID data. The BIR submitted by the user is compared to the retrieved reference BIR. User verification is based upon this comparison. See Brown et al. column 4, lines 5-6 and column 5, lines 13-17. In other words, the verification process of Brown et al.'s biometric authentication system involves obtaining object ID data (user ID and password) to verify a person's identity incident to scanning, wherein the verification means verifies identity by comparing a combination of the extracted biometric information (BIR) and the object ID data with a combination of the corresponding reference biometric information and reference ID data.

35. While Brown et al.'s teachings are directed more to an authentication system implemented in a computer network environment, it should be clear that such a system may just as well be implemented as a unitary, localized system. Implementing this system as such or incorporating these teachings into a greater unitary, localized system would be well within the capabilities of one of ordinary skill in the art. Furthermore, note that Brown et al. do not constrain their system to operate on any specific biometric source (e.g. see Brown et al. column 4, lines 63-65).

Taking this into account and the fact that the biometric authentication system of Brown et al. and the iris verification system of Flom et al. are principally the same in structure and function, it would be straightforward for one of ordinary skill in the art to add an object ID data obtaining means, such as that of Brown et al., the associated object ID verification, and reference database structure to the iris identification system of Flom et al. The motivation to do so is to provide an initial identification of the user via the user ID and password. This allows, among other things, the detection of whether biometric information indeed exists for the user (as shown in reference number 305 of Brown et al. Fig. 3). Moreover, employing ID data in this manner obviates the need to laboriously compare the user-supplied biometric information with all database records by providing an intuitive, simple, and efficient means to index and parse the database of reference biometric information. Therefore, given the advantages and relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to add an object ID data obtaining means, such as that of Brown et al., the associated object ID verification, and reference database structure to the iris identification system of Flom et al. In doing so, one would obtain an identity verification apparatus in accordance with claim 12.

36. *The following is in regard to Claim 13.* As shown above, the teachings of Flom et al. and Brown et al. can be combined in such a way as to satisfy all limitations of claim 12. As mentioned above, the verification process taught by Brown et al. involves retrieving reference biometric information (BIR) from a database, consisting of a plurality of reference BIRs (Brown et al. column 4, lines 1-3) according to the supplied ID data. The BIR submitted by the user is compared to the retrieved reference BIR. User verification is based upon this comparison. See Brown et al. column 4, lines 5-6 and column 5, lines 13-17. In this way, the identity verification system, obtained by combining the teachings of Flom et al. and Brown et al. in the manner described above, is an apparatus, in accordance with claim 12, wherein the verification means specifies (retrieves) one from among a plurality of combinations of reference biometric information (BIR) and reference ID data, which corresponds with the object ID data, and verifies identity by comparing the specified reference biometric information with the extracted biometric information. Such an identity verification apparatus satisfies all limitations of claim 13.

37. Claims 14-17 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Pare et al. (U.S. Patent 5,802,199).

38. *The following is in regard to Claim 14.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. further propose that the reference biometric descriptors be stored on a storage means. See Flom et al. column 2, lines 46-52. Though not explicitly shown by Flom et al., such storage means inherently comprises a reference information updating means for somehow updating the stored biometric information. However, Flom et al. do not show or suggest that this updating means should replace reference biometric information.

39. Pare et al. disclose an identification computer system for determining an individual's identity from comparison of previously recorded biometric samples (Pare et al. column 3, lines 45-49). This system includes a storage means (e.g. the databases shown in Pare et al. Figs. 8-9) for storing reference biometric information and a reference information updating means for replacing reference biometric information stored by the storage means with biometric information extracted by the verification means. See Pare et al. column 10, lines 15-35. Specifically, Pare et al. show that records of biometric information are purged from the database (e.g. IBD 44 in Fig. 8 of Pare et al.), by a purging engine, (see Pare et al. column 4, lines 33-35 and Pare et al. column 10 lines 21-25) and new reference biometric records replace these during the verification process (Pare et al. column 10, lines 15-20). This purging and adding process represents a reference information updating means for replacing reference biometric information, stored by the storage means, with biometric information extracted by the verification means.

40. While Pare et al.'s teachings are directed more to an identification computer system implemented in a computer network environment, it should be clear that such a system may just as well be implemented as a unitary, localized system. Implementing this system as such or incorporating these teachings into a greater unitary, localized system would be well within the capabilities of one of ordinary skill in the art. Furthermore, note that Pare et al. do not constrain their system to operate on any specific biometric source (e.g. see Pare et al. column 9, lines 43-45). Taking this into account and the fact that the identification computer system of Brown et al. and the iris verification system of Flom et al. are principally the same in structure and function, it would be straightforward for one of ordinary skill in the art to incorporate the reference updating means, as taught by Pare et al., into the iris identification system of Flom et al. Providing a means to update records is an essential function to any database. For example, such an updating means allows one to effectively manage the size of the database(s), as well as the

redundancy and accuracy of the biometric data contained therein. This, in turn, improves the accuracy of the verification process and its overall speed. Therefore, taking into account the demonstrated utility of an updating means, such as that of Pare et al., the relative ease of integrating such an updating means into an identity verification system, and, moreover, the general requirement of any apparatus, utilizing a storage means, to provide a means to update data records stored thereon, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to supplement the reference-biometric-information storage means of Flom et al.'s iris verification system with a reference information updating means for replacing reference biometric information stored by the storage means with biometric information extracted by the verification means. In making such a provision, one obtains an identity verification apparatus, in accordance with claim 2, that satisfies all limitations of claim 14.

41. *The following is in regard to Claim 15.* As shown above, the teachings of Flom et al. and Pare et al. can be combined in such a way as to satisfy all limitations of claim 14. Pare et al. also teach replacing biometric records upon the expiration of a predetermined time period from the most recent identification of an individual. See Pare et al. column 10, lines 21-38. As discussed above, the purged records are replaced by newly reference biometric records replace these during the verification process (see Pare et al. column 10, lines 15-20). This exploits the temporal locality in the biometric information, that is, biometric information that is used frequently (associated with frequent users of the system) is more likely to be referenced and is, therefore, retained locally, whereas less frequently used information is purged. This typically reduces the time to parse the database. See Pare et al. column 10, lines 39-43. In this way, the teachings of Flom et al. and Pare et al., when combined in the manner discussed above, produce an identity verification apparatus that satisfy all limitations of claim 15.

42. *The following is in regard to Claim 16.* Flom et al. disclose an iris recognition (based on the biometrics of the human iris) comprising the following:

a. A scanning means (i.e. the scanning camera 180 depicted in Flom et al. Fig. 10) for obtaining an image of the iris (note that, henceforth in this document, the iris image will be referred to interchangeably as the object image when the distinction as such is unimportant) by scanning an eye (note that, henceforth in this document, the eye will be referred to interchangeably as the body

part when the distinction as such is unimportant) of a person without physical contact. Notice, from Flom et al. Fig. 8, for example, that the scanning of the iris occurs without physically contacting the eye.

b. An image display means (i.e. display screen 86 shown in Fig. 9 of Flom et al.) for displaying the object image to the person. See Fig. 9 of Flom et al. and column 9, lines 27-65.

c. A guide display means (i.e. display screen 86 shown in Fig. 9 of Flom et al.) for displaying a guide layered over the object image (i.e. reference number 30 in Flom et al. Fig. 9), the guide showing an outline of the body part in proper position. Reference number 30 is an outline of the pupil of the subject's eye. The peripheral points 88a and the center point 88b are used to align the subject's eye in a standardized position. This is discussed in Flom et al. column 9, lines 23-41.

d. A judgment means for judging whether the object image was scanned in the proper position. In the iris recognition system of Flom et al., the pupil outline 30 superimposed upon the image display screen 86, as illustrated in Flom et al. Fig. 9, allows the operator to judge whether the subject's eye, and hence the subject's iris, is in the proper, standardized position. In this way, these items (i.e. pupil outline 30 and display screen 86) taken together represent a judgment means for judging whether the iris was scanned in the proper position.

e. Biometric information extracting means for extracting biometric information describing a form characteristic of the body part from the object image, if in the proper position, (e.g. Flom et al. Fig. 7 step 64), and verifying identity by comparison with stored reference biometric information (e.g. Flom et al. Fig. 4 step 66). Refer also to Flom et al. Fig. 12.

f. A biometric information storage means (henceforth referred to, interchangeably, as a biometric database) for storing a plurality of reference biometric information. Flom et al. propose that the reference biometric descriptors be stored on a storage means. See Flom et al. column 2, lines 46-52.

g. A verification means for verifying identity by comparing captured biometric information with reference biometric information stored in the biometric information storage means. See, for example, Fig. 62, step 62, Fig. 7, and Flom et al. column 2, lines 46-52.

Flom et al., however, do not show or suggest that their iris verification system consist of a verification server connected to a verification terminal connected via a network, wherein the aforementioned scanning means, image display means, guide means, judgment means, and biometric extraction means resides on the verification terminal, and the biometric database and verification means resides on the verification server.

43. Pare et al. show a network-based biometric identification system consisting of at least one terminal (e.g. Local Computer 34 in Pare et al. Fig. 8) and a server (e.g. Master Computer 10 in Pare et al. Fig. 8). Each of the terminals includes a biometric scanner (e.g. reference number 36 in Pare et al. Fig. 8) or biometric input apparatus (Pare et al. column 12, lines 40-69) for extracting biometric information. The biometric information is relayed, via a network connection, to the server, which includes a database of biometric information (e.g. IBD 30 in Pare et al. Fig. 8). Notice from the flow diagram in Master Computer 10 in Pare et al. Fig. 8 that a verification process is executed on the server and the result is relayed to the client. This verification is based on a comparison (e.g. step 28 in Pare et al. Fig. 8) between the transmitted biometric information and the reference biometric data stored in the biometric database.

44. Implementing the iris verification system of Flom et al. as a network-based system would be a simple undertaking for one of ordinary skill in the art, given the teachings of Pare et al. The advantages of using a network - based implementation, as opposed to unitary, localized implementations are many. In this case, an obvious advantage of the network-based approach is the reduction in overall cost of the verification system. The network-based verification system reduces cost by reducing the storage requirements of the client terminals, which may be numerous. Therefore, given that Pare et al.'s successful application of a network-based approach to implementing a biometric identification system, and in an effort to reduce the cost, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to apply a implement the iris verification system of Flom et al. as a network-based system, where, as taught by Pare et al., the verification terminal includes a biometric scanning means and biometric information extraction means and the verification server includes a biometric database and a verification means that compares reference biometric information to the extracted biometric information, transmitted to the server vie a network connection. Furthermore, to achieve the greatest utility from such a combination, it would have also been obvious to have the display means, guide means, and judgment means of Flom et al.'s verification system reside on the verification terminal, thereby, providing the user with visual cues in

properly aligning the iris, or other body part. Combining the teachings of Flom et al. and Pare et al., in this manner, yields an identity verification apparatus in accordance with claim 16.

45. *The following is in regard to Claim 17.* As shown above, the teachings of Flom et al. and Pare et al. can be combined in such a way as to satisfy all limitations of claim 16. Note that the verification terminal(s) (e.g. Local Computer 34 in Pare et al. Fig. 8) of Pare et al.'s identification system further includes an ID data obtaining means (e.g. keypad 38 in Pare et al. Fig. 8) for obtaining ID data (Personal Identification Code (PIC) – Pare et al. column 3, lines 45-51) prior to and concomitantly to biometric scanning. See, for example, Pare et al. Fig. 8. This terminal(s) receive (download) from the verification server (e.g. Master Computer 10 in Pare et al. Fig. 8) reference biometric information corresponding to the ID data. See, for example, Pare et al. column 10 lines 15-20). Additionally, the verification terminals have a verification process that is executed locally. This is illustrated, for example, in the flow diagram depicted in Local Computer 34 in Pare et al. Fig. 8. This process involves the comparison (e.g. comparison 42 of Fig. 8 of Pare et al.) of the extracted biometric information with the reference information received from the verification server. See Pare et al. column 9, lines 59-67 to column 10 lines 1-20.

46. The verification server (e.g. Master Computer 10 in Pare et al. Fig. 8) of Pare et al.'s biometric identification system includes an ID data storage (i.e. a personal identification group database – Pare et al. column 3, lines 56-58) means for storing reference ID data corresponding to each of the plural sets of reference biometric information stored in the biometric database. The verification server receives ID data from the terminal(s) indicating the corresponding biometric information record in the server's biometric database. See Pare et al. column 10, lines 5-10. The verification server relays the corresponding reference biometric information to the verification terminal. See Pare et al. column 10, lines 15-20. . In this way, the identity verification apparatus obtained by combining the teachings of Flom et al. and Pare et al., in the manner discussed above, conforms to all limitations of claim 17.

47. *The following is in regard to Claim 26.* Note that Pare et al. Figs. 3-4 and column 13, lines 30-35 are suggestive of Pare et al.'s network-based identification system being used as an electronic transaction system. Also note that, other than distinguishing itself as an electronic transaction system based on identity verification by biometrics, claim 26 puts forth substantially the same subject matter as claimed in claim 16. Therefore, with regard to claims 26, remarks analogous to those presented above with regard to claim 16 and are applicable. With regard to the information describing the electronic transaction, Pare et al. suggest that this information (e.g. financial

information) be transmitted to the verification server from the verification terminal and vice versa. See Pare et al. column 13, lines 45-52 and column 14, lines 12-26. The transaction proceeds depending on the outcome of the comparison of the reference biometric information with the transmitted biometric information. See Pare et al. column 14, lines 12-26. Finally, it is inherent that any electronic transaction system to have a receiving means for receiving a request from an operator to make an electronic transaction. Therefore, given the discussion above with respect to clam 16, the identity verification apparatus obtained by combining the teachings of Flom et al. and Pare et al., in the manner discussed above, addresses to all limitations of claim 26.

48. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Musgrave et al. (U.S. Patent 6,377,699).

49. *The following is in regard to Claim 19.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in a portable phone.

50. Musgrave et al. describe a portable phone that utilizes iris verification. See Musgrave et al. Fig. 9 and column 3, lines 63-64. It would be a simple undertaking for one of ordinary skill in the art to use the iris verification of Flom et al. instead of that of Musgrave et al. in the portable phone because of their inherent functional and structural similarities. The iris verification of Flom et al. would advantageously provide visual cues (via the image display and guide display means) for aligning the iris for proper image capture. This would result in more accurate verification. Given this advantage and the relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system of Flom et al. instead of that of Musgrave et al. in the portable phone. In doing so, one would obtain a portable phone that satisfies all limitations of claim 19.

51. Claims 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Oda et al. (U.S. Patent 6,591,001).

52. *The following is in regard to Claim 20.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in a personal computer (PC).

53. Oda et al. describe a PC with an iris-capturing device for the purposes of user verification. See Oda et al. Fig. 1 and column 2, lines 18-26. It would be a simple undertaking for one of ordinary skill in the art to use the iris verification and associated iris-capture components of Flom et al. instead of those of Oda et al. in the PC because of their inherent functional and structural similarities. An iris verification system, as taught by Flom et al., would advantageously include an automatic alignment system. See Flom et al. column 10, lines 56-65. This eliminates the need for the user to properly position his/her eye. Given this advantage and the relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system and associate iris-capturing components of Flom et al. instead of those of Oda et al. in the PC. In doing so, one would obtain PC that satisfies all limitations of claim 20.

54. Claims 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Cambier et al. (U.S. Patent 6,532,298).

55. *The following is in regard to Claim 21.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in a building management system which controls the entry or exit of persons to a building, comprising a control means for unlocking a door when identity is verified by the identity verification apparatus.

56. Cambier et al. describe a door locking mechanism with that utilizes iris verification. Unlocking of the door (which presumably is part of a building) occurs only when the iris of the subject has been identified. See Cambier et al. column 2, lines 9-33. It would be a simple undertaking for one of ordinary skill in the art to use the iris verification of Flom et al. instead of that of Cambier et al., used in their locking mechanism, because of their inherent functional and structural similarities. The iris verification of Flom et al. would advantageously provide visual cues (via the image display and guide display means) for aligning the iris for proper image capture. This would result in more accurate verification. Given this advantage and the relative ease of such a modification, it

would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system of Flom et al. instead of that of Cambier et al. in the door locking mechanism (building management system) of Cambier et al. In doing so, one would obtain a building management system that satisfies all limitations of claim 21.

57. Claims 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Hsu et al. (U.S. Patent 6,100,811).

58. *The following is in regard to Claim 22.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in a motorized vehicle comprising a control means for starting the vehicle when the identity verification apparatus verifies the user's identity.

59. Hsu et al. disclose an automobile control apparatus that allows a user to entry to or start a vehicle based on a verification of his/her supplied biometric information. See Hsu et al. column 4, lines 26-41. It would be a simple undertaking for one of ordinary skill in the art to use the iris verification of Flom et al. instead of the fingerprint verification of Hsu et al. in the control apparatus of Hsu et al. because, being biometric verification apparatuses, they share certain functional and structural similarities. Furthermore, it is well known that the human iris provides an extremely effective contact-less means to identify an individual. In addition, the iris verification of Flom et al. would advantageously provide visual cues (via the image display and guide display means) for aligning the iris for proper image capture. This would result in more accurate verification. Given these advantages and the relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system of Flom et al. instead of the fingerprint verification of Hsu et al. in the automobile controlling apparatus of Hsu et al. Such a device could, in turn, be used in a vehicle to provide a keyless and highly secure means to access the vehicle. In doing so, one would obtain a motorized vehicle that satisfies all limitations of claim 22.

60. Claims 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Saito et al. (U.S. Patent Application Publication 2002/0034321)

61. *The following is in regard to Claim 23.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in an automatic vending machine comprising a control means for dispensing a specified product when identity is verified by the identity verification system.

62. Saito et al. discusses the application of a biometric identity verification apparatus to a vending machine in order to allow an operator access to the various products contained therein. See Figs. 3 and 24 of Saito et al.

63. It would be a simple undertaking for one of ordinary skill in the art to use the iris verification of Flom et al. instead of the fingerprint verification of Saito et al. in a vending machine, such as that shown in Fig. 24 of Saito et al., because, as biometric verification apparatuses, they share certain functional and structural similarities. This is evident from Saito et al. Fig. 3. . Furthermore, it is well known that the human iris provides an extremely effective contact-less means to identify an individual. In addition, the iris verification of Flom et al. would advantageously provide visual cues (via the image display and guide display means) for aligning the iris for proper image capture. This would result in more accurate verification. Given these advantages and the relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system of Flom et al. instead of the fingerprint verification apparatus of Saito et al., in a vending machine, such as that shown in Fig. 24 of Saito et al. In doing so, one would obtain an automatic vending machine that satisfies all limitations of claim 23.

64. Claims 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Doster (U.S. Patent 5,956,122).

65. *The following is in regard to Claim 24.* As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in an

automatic teller machine (ATM) comprising a deposit/withdrawal processing means for processing a deposit or withdrawal transaction when identity is verified by the identity verification apparatus.

66. Doster discusses the usage of an iris recognition apparatus in an ATM. See Doster Figs. 1-2. As with any ATM, deposit and withdrawal requests are made by a customer and some deposit/withdrawal request processing means handles these requests. In Doster's invention, the customer only gains access to these functions when his/her iris has been recognized. See paragraph 1 of Doster's Detailed Description. In this manner, deposit and withdrawal requests are processed only when the customer's biometric information (iris) has been verified.

67. It would be a simple undertaking for one of ordinary skill in the art to use the iris verification of Flom et al. instead of the iris recognition apparatus of Doster in an ATM, as depicted in Doster Fig. 1, because, being iris verification apparatuses, they share several inherent functional and structural similarities. The iris verification of Flom et al. would advantageously provide visual cues (via the image display and guide display means) for aligning the iris for proper image capture. This would result in more accurate verification. Given this advantage and the relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system of Flom et al. instead of the iris recognition apparatus of Doster in an ATM, such as the one depicted in Doster Fig. 1. In doing so, one would obtain an ATM that satisfies all limitations of claim 24.

68. Claims 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flom et al., in view of Pare et al. (U.S. Patent 6,662,166).

69. *The following is in regard to Claim 25.* . As shown above, Flom et al. disclose an identity verification apparatus that conforms to claim 2. Flom et al. do not, however, suggest the usage of such an apparatus in a point-of-sale (POS) terminal comprising a deposit/withdrawal processing means for processing a deposit or withdrawal transaction when identity is verified by the identity verification apparatus.

70. Pare et al. discuss the usage of a biometric verification apparatus in a POS terminal (e.g. POS terminal 1 in Pare et al. Fig. 1) where financial transactions, including deposits and withdrawals (purchases), are processed when a customer's biometric information has been verified. See paragraph 1 of Pare et al.'s Detailed Description. A means

to process user requests for these financial transactions (e.g. withdrawals and deposits) is inherent to any POS system.

71. While Pare et al.'s teachings are directed more to an identification computer system implemented in a computer network environment, it should be clear that such a system may just as well be implemented as a unitary, localized system. Alternatively, the iris verification system of Flom et al. may be implemented as a network-based system by separating the various verification operations according to Pare et al.'s teachings. Implementing a POS terminal and system in either way would be well within the capabilities of one of ordinary skill in the art. Furthermore, note that Pare et al. do not constrain their system to operate on any specific biometric source (see Pare et al. column 8, lines 10-13). Therefore, it would be straightforward for one of ordinary skill in the art to use the iris verification system of Flom et al., as a stand-alone system or adopted to work in a network-based environment, instead of the biometric verification system of Pare et al. in a POS terminal, such as that of Pare et al. Among other things, the iris verification taught by Flom et al. would advantageously provide visual cues (via the image display and guide display means) for aligning the iris for proper image capture. This would result in more accurate verification. Given these advantages and the relative ease of such a modification, it would have been obvious to one of ordinary skill in the art, at the time of the applicant's claimed invention, to use the iris verification system of Flom et al., as a stand-alone system or adopted to work in a network-based environment, instead of the biometric verification system of Pare et al. in a POS terminal, such as that of Pare et al. In doing so, one would obtain a POS terminal that conforms to the limitations of claim 25.

Citation of Relevant Prior Art

72. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

[1] *U.S. Patent 5,291,560. Biometric Personal Identification System Based on Iris Analysis.* Daugmann, 1994. Duagmann gives a thorough discussion about using the human iris as a means of identification. Daugmann, like Flom et al., uses an image of the iris with an

superimposed target outlining the iris. Daugmann also suggests capturing multiple images, at regularized time intervals, to detect changes in the size of the pupil. As with Steinberg et al. and the applicant, this is done to ensure biometric samples are taken from a living eye. The general method of verifying a subject's iris is also set forth in this patent.

[2] *U.S. Patent 5,177,802. FINGERPRINT INPUT APPARATUS.* Fujimoto et al., 1993. Fujimoto et al. disclose a contact-less fingerprint scanning means that uses an auto-focusing image pickup device (camera).

[3] *U.S. Patent 6,404,904. System for the Touchless Recognition of Hand and Finger.* Eignenhammer et al., 2002. Eignenhammer disclose a contact-less fingerprint scanning and recognition means.

[4] *U.S. Patent 4,936,680. Method of, and Apparatus for Edge Enhancement of Fingerprint Minutia.* Henkes et al. 1990. Henkes et al. disclose a contact-less fingerprint scanning means.

[5] *U.S. Patent 5,956,415. Enhanced Security Fingerprint Sensor Package and Related Methods.* McCalley et al. 1999. McCalley et al. teach displaying an image of captured biometric sample – in this case, a fingerprint – to the user as well as guide used to indicate the proper positioning of the biometric source (e.g. a finger).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Siangchin whose telephone number is (703)305-7569. The examiner can normally be reached on 9:00am - 5:30pm, Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Amelia Au can be reached on (703)308-6604. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kevin Siangchin

Examiner
Art Unit 2623

ks – 03/15/04

AMELIA M. AU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600